Министерство образования и науки Российской Федерации

(МИНОБРНАУКИ РОССИИ)

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (ТГУ)

Институт прикладной математики и компьютерных наук

Кафедра защиты информации и криптографии

**КУРСОВАЯ РАБОТА**

БИБЛИОТЕКА ДЛЯ РАБОТЫ С БУЛЕВЫМИ ФУНКЦИЯМИ ДЛЯ ЯЗЫКА ПРОГРАММИРОВАНИЯ LYAPAS

Муругов Михаил Алексеевич

Руководитель

канд. физ.-мат. наук, доцент

\_\_\_\_\_\_\_\_\_\_\_\_И.А.Панкратова «\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_201\_\_\_г.

Студент группы № 1155

\_\_\_\_\_\_\_\_\_\_\_\_\_М.А.Муругов

Томск 2018

ОГЛАВЛЕНИЕ

Введение………………………………………………………………………………………….2

1 Описание алгоритмов на математическом языке……………………………………………3

* 1. Принадлежность булевой функции к классу ……………………………………………3
  2. Принадлежность булевой функции к классу ……………………………………………..
  3. Преобразование Мёбиуса булевой функции………………………………………………...
  4. Принадлежность булевой функции к классу линейных булевых функций………………...
  5. Принадлежность булевой функции к классу самодвойственных булевых функций……...

2 Программные реализации

2.1

3 Экспериментальные данные

Заключение

Список литературы

Приложения

ВВЕДЕНИЕ

Целью этой курсовой работы было написание библиотеки для работы с булевыми функциями для языка программирования LYaPAS. В дальнейшем планируется, что эта библиотека будет использоваться для реализации криптографических алгоритмов и прочих нужд.

ОПИСАНИЕ АЛГОРИТМОВ НА МАТЕМАТИЧЕСКОМ ЯЗЫКЕ

Принадлежность булевой функции к классу

**Определение.** Булева функция *сохраняет константу 0* (*принадлежит классу )*, если на наборе из всех нулей функция принимает значение нуль.

Алгоритм:

Вход: – булева функция

Выход: “ принадлежит классу ?”

Шаг 1) Если , то ответ “Да”

Иначе ответ “Нет”

Принадлежность булевой функции к классу

**Определение.** Булева функция *сохраняет константу 1* (*принадлежит классу* ), если на наборе из всех единиц функция принимает значение единица.

Алгоритм:

Вход: – булева функция

Выход: “ принадлежит классу ?”

Шаг 1) Если , то ответ “Да”

Иначе ответ “Нет”

Преобразование Мёбиуса булевой функции

**Определение.** *Положительной конъюнкцией* называется элементарная конъюнкция, не содержащая инверсий переменных. Договоримся обозначать положительную конъюнкцию через .

**Определение.** *Полиномом Жегалкина*, или *алгебраической нормальной формой (АНФ)*, булевой функции называется дизъюнкция с исключением различных положительных конъюнкций переменных из множества , то есть формула вида задающая функцию .

**Определение.** Преобразованием Мёбиуса называется функция , где – множество всех булевых функций от переменных. С помощью преобразования Мёбиуса решается задача построения АНФ булевой функции, и вычислить его значения для функции можно по формуле . Рассмотрим возможный способ выполнения этого вычисления.

**///Убрать способ? Написать сразу рекурсивный алгоритм?///**

Построим матрицу отношения предшествования булевых векторов , строкам и столбцам которой сопоставлены булевы векторы длины и

Например, ;

Нетрудно убедиться, что и , где – вектор-столбец значений функции . Если и — соответственно младшая и старшая половины вектора значений , то по формуле получим следующую рекурсивную формулу:

.

На «дне» рекурсии для функции от одной переменной

На основании этого способа преобразование Мёбиуса реализовано программно.

Принадлежность булевой функции к классу линейных булевых функций

**Определение.** *Длиной* булева вектора назовем количество его компонент, а *весом* вектора – количество компонент, равных единице

Длину булева вектора в дальнейшем будем обозначать . Запись , где – булева функция, будет обозначать длину вектора её значений.

Вес булева вектора в дальнейшем будем обозначать . Запись , где – булева функция, будет обозначать вес вектора её значений.

**Определение.** *Длиной полинома Жегалкина назовем* количество конъюнкций в полиноме, а его *степенью* – наибольший из рангов конъюнкций, входящих в полином.

**Определение.** Полином Жегалкина называется *линейным*, если его степень не превышает единицы.

**Определение.** Булева функция называется *линейной* (*принадлежит классу* ), если ее полином Жегалкина линеен.

Алгоритм:

Вход: – булева функция

Выход: “ – линейна?”

Шаг 1)

Шаг 2)

Шаг 3) Для всех векторов таких, что и

Шаг 3.1)

Шаг 4) Если , то ответ “Да”

Иначе ответ “Нет”

Принадлежность булевой функции к классу самодвойственных булевых функций

**Определение.** Булева функция называется *двойственной булевой функции* , если она получена из инверсией всех аргументов и самой функции, то есть .

**Определение.** Булева функция  *самодвойственна* (*принадлежит классу* ), если она равна двойственной себе функции, то есть .

**////Нужно ли вводить определение для reverseBits?///**

Алгоритм:

Вход: – булева функция

Выход: “ – самодвойственна?”

Шаг 1) – младшая половина вектора значений

– старшая половина вектора значений